SOFTWARE SECURITY FOR U-NII DEVICES

Date: 2015/4/23

FCC ID: XU8TEW817DTR

Pursuant to FCC Part 15E 15.407(i) and KDB 594280 D02 U-NII Device Security, applicant must describe the overall security measures and systems that ensure that only:

1. Authenticated software is loaded and operating the device.
2. The device is not easily modified to operate with RF parameters outside of the authorization

The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements.

SOFTWARE SECURITY DESCRIPTION / General Description	
1.	Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security.
	Firmware updates may be downloaded from website at http://www.trendnet.com/support and installed through the device's web based system interface.
2	Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?
	All the radio frequency parameters are transmit power, operating channel, modulation type. Only authorized parameters are available and can be set in the software.
3	Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification.
	TRENDnet firmware will check model name, hardware version and region code. If invalid, that will not accept the FW upgrading successfully.
4	Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate
	TRENDnet firmware has a kernel signature to check firmware is legitimate.
5	Describe in detail any encryption methods used to support the use of legitimate software/firmware
	Firmware image is not encrypted but compressed.
6	For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation?
	The device is not only a master but also a client(with passive scanning).

SOFTWARE SECURITY FOR U-NII DEVICES

Date: 2015/4/23

SOFTWARE SECURITY DESCRIPTION / Third-Party Access Control	
1.	Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.
	The AP sold to the US cannot be operated on any other country or domains. This is locked into the manufacturing data and cannot be changed.
2	What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from “flashing” and the installation of third-party firmware such as DD-WRT
	The devices are HW configured to only accept US firmware loads only at the time of manufacture, and not changeable.
3	For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures fully comply with these software security requirements for U-NII devices. If the module is controlled through driver software loaded in the host, describe how the drivers are controlled and managed such that the modular transmitter parameters are not modified outside the grant of authorization.
	The device is not a modular device.

SOFTWARE SECURITY FOR U-NII DEVICES

Date: 2015/4/23

In addition to the general security consideration, for devices which have “User Interfaces” (UI) to configure the device in a manner that may impact the operational parameter, the following questions shall be answered by the applicant and the information included in the operational description. The description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01

SOFTWARE SECURITY DESCRIPTION / USER CONFIGURATION GUIDE			
1.	To whom is the UI accessible? (Professional installer, end user, other.)		
	The UI is accessible to the end user.		
	a	What parameters are viewable to the professional installer/end-user?	
		The end user can view the RF channel and Tx power levels.	
	b	What parameters are accessible or modifiable to the professional installer?	
		The RF channel can only be set to FCC approved channels. The TX power level can be set up to the approved RF power levels (or less).	
		(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
			Yes, all radio parameters are limited by SW settings pre-determine by the FCC radio regulatory approval process.
		(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?
			The radios are configured at manufacturing to be US only and only TRENDnet US FW loads can be installed. These loads control the limits of the operation of the radio.
	c	What configuration options are available to the end-user?	
		The end user can change the RF channel and Tx power levels.	
		(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
			Yes, all radio parameters are limited by SW settings pre-determine by the FCC radio regulatory approval process.
		(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?
			The radios are configured at manufacturing to be US only and only TRENDnet US FW loads can be installed. These loads control the limits of the operation of the radio.
	d	Is the country code factory set? Can it be changed in the UI?	
		Yes the country code is factory set. It cannot be changed in the UI.	
		(1)	If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
			The radios are configured at manufacturing to be US only and only TRENDnet US FW loads can be installed.
	e	What are the default parameters when the device is restarted?	
		The device goes to a default (approved) Tx channel and power level based on factory country setting.	
2	Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02		
	This approval is for UNII-3 band and this KDB applies only to UNII-2A and UNII-2C.		
3	For a device that can be configured as a master and client (with active or passive scanning),if this is user configurable, describe what controls exist, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?		

SOFTWARE SECURITY FOR U-NII DEVICES

Date: 2015/4/23

	The device is not only a master but also a client. There are two master modes which could be switched by hardware switch. Other two client modes should be switched by software.
4	For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a))
	The user select which mode at UI, the internal wireless mode flag ensure compliance operation.